UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,986	06/30/2000	Jin Su	10559/214001/P8707	1439

21552 7590 08/25/2005

MADSON & METCALF
GATEWAY TOWER WEST
SUITE 900
15 WEST SOUTH TEMPLE
SALT LAKE CITY, UT 84101

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,986	SU ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-27* is/are pending in the application.

4a) Of the above claim(s) *14 and 15* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-13 and 16-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *14 and 15* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 6/3/2005 was received and considered.

2. Claims 8-27 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 8-27 have been considered but are moot in view of the new ground(s) of rejection.

4. Regarding claims 14-15, by Applicant's amendment of 6/3/2005, the Examiner has appreciated that the invention claimed in claims 14-15 is substantially distinct from the invention described in claims 8-13 and 16-27. Therefore, claims 14-15 are restricted by original presentation, as described below.

5. Applicant's response (§III - §V) suggests that the references of record do not disclose or teach a security extension as amended. However, Elgamal teaches an extension in both the client and server, for the purposes of security in the form of an SSL extension that handles the creation, etc. of SSL connections (see for example Fig. 11) and hence performs the challenge of Elgamal's invention as it is performed with respect to the server (Fig. 11).

Election/Restrictions

6. Newly submitted claims 14-15 are directed to an invention that is independent or distinct from the invention originally claimed for the following reasons: Group I, claims 14-15 are directed to determining the identity of a client and exchanging a symmetric key generating by a security filter using the public key method (not requiring verifying a certificate and challenge

response mechanism), classified in class 380, subclass 285 whereas Group II, claims 8-13 & 15-27 are directed to authentication using a certificate and performing a challenge generated by a security extension (not requiring exchanging a symmetric key using the public key method), classified in class 713, subclass 175. Groups I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, Group I has separate utility such as exchanging a symmetric key without prior negotiation, whereas Group II can be used to authenticate users. See MPEP § 806.05(d).

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 14-15 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 8-12, 16-22, 24-26 & 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,657,390 to Elgamal et al. (**Elgamal**) in view of U.S. Patent 6,816,900 to Vogel et al. (**Vogel**) and "Single Sign-On Using Cookies for Web Applications" by **Samar**.

Regarding claims 8, 12, 16-17, 24, 26 & 27, Elgamal discloses submitting a request to access a node/open SSL connection using CLIENT_HELLO (Figs. 4-6), directing to submit a certificate (server certificate, col. 22, line 56 – col. 23, line 8 and client certificate, col. 29, lines 29-61), performing a challenge/CERTIFICATE-CHALLENGE-DATA (col. 29, line 34), wherein the challenge is generated by a security extension/SSL in a server (Fig. 11) and generating a response (server, SERVER-VERIFY col. 28, lines 28-64 and client, RESPONSE-DATA col. 30, lines 7-8 & lines 27-50) to the challenge. Elgamal lacks disclosure of implementation-specific verification of the submitted certificate. However, Vogel teaches that in an SSL session, a certificate is verified using a root certificate/trusted certificate to prove that the server is approved for secure connections (col. 1, lines 30-40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Elgamal to verify the client/server certificates in Elgamal's SSL protocol with a trusted certificate/root certificate in the browser. One of ordinary skill in the art would have been motivated to perform such a modification to prove that the server is approved for secure connections, as taught by Vogel (col. 1, lines 30-40). As modified, Elgamal lacks saving the response (RESPONSE-DATA or SERVER-VERIFY) as a named cookie. However, Samar teaches that storing response data (cookie id and cookie integrity check) (Fig. 1 & §6.1.2) is advantageous for single sign-on because no extra software has to be installed and it is

independent from the authentication mechanism (§4). Samar teaches a verifier authenticating a requesting entity, but rather than ending the process after the authentication, a security token/cookie is created and sent from the verifier to the entity to be stored (§3.1 & Fig. 1). The web server challenges the cookie server; the cookie server responds to the challenge and stores the response as a named cookie (sends brownie + cookie back to the authenticating web server and the cookie is sent back to the browser) (Fig. 1 & §6.1). This allows for fast authentication in the future (§1, ¶3, §3.1 & §6.1) because the stored response can be sent along with further requests. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the authentication scheme used by Elgamal with the client-authenticating SSO architecture to store a response (RESPONSE-DATA or SERVER-VERIFY) as a named cookie. One of ordinary skill in the art would have been motivated to perform such a modification to enable single sign-on without the need for extra software or specific authentication mechanisms, as taught by Samar (Fig. 1 & §4).

Regarding claims 9 & 25, Elgamal, as modified above, discloses using the cookie/response as a security token (Samar, §6.1).

Regarding claim 10, Elgamal, as modified above, discloses the security token being used to propagate initial authentication (Samar, §6.1).

Regarding claim 11, Elgamal, as modified above, discloses creating a connection session if the certificate is valid (Fig. 4 & col. 8, lines 54-61).

Regarding claim 18, Elgamal lacks creating a new authentication session with the authentication token. However, Samar discloses a centralized login server approach to single sign-on where an initial web server redirects a client to a new web server that has access to a

cookie server (Fig. 2). The new web server then redirects the client back to the first server with the cookie where the web server verifies the cookie and returns a session cookie (creating and registering a new authentication session). The initial web server validates the new authentication session using the authentication token/cookie (Fig. 2 & §8). The benefit of the centralized login server is that all authentication information for the user is consolidated (§8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to create and register a new authentication session. One of ordinary skill in the art would have been motivated to perform such a modification to enable the consolidation of all authentication information, as taught by Samar (Fig. 2 & §8).

Regarding claim 19, Elgamal lacks explicitly indicating a failure status to a client if verification fails. However, Elgamal discloses that error handling in SSL works in such a way that when an error is detected, the detecting party sends a message to the other party, including a bad certificate error (col. 20, lines 4-10 & lines 25-32). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made modify Elgamal to explicitly send the client a message indicating a failure status to the client if verification of the client's certificate fails. One of ordinary skill in the art would have been motivated to perform such a modification to indicate to the client if verification of its certificate fails, as taught by Elgamal (col. 20, lines 4-10 & lines 25-32).

Regarding claim 20, Elgamal, as modified above, discloses the challenge being a random number (col. 7, lines 13-19).

Regarding claim 21, Elgamal, as modified above, discloses receiving an address/URL of a node and checking to determine if the address is protected (SSL to be used for information retrieval) (Fig. 12A).

Regarding claim 22, Elgamal lacks determining if the authentication token is already present. However, Samar teaches that SSO is useful so that users to not have to enter usernames and passwords many times per day (§1). Samar further teaches that in a centralized login server approach, a server first must check to see if a cookie was presented (authentication token already present) (§8 & Fig. 2) (otherwise the system would not be SSO). The centralized approach brings the benefit of authentication and management centrality (§8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine if the authentication token is already present. One of ordinary skill in the art would have been motivated to perform such a modification to implement an SSO system to prevent repeated username and password combination uses, as taught by Samar (§1, §8 & Fig. 2).

9. Claim 13, is rejected under 35 U.S.C. 103(a) as being unpatentable over **Elgamal** in view of **Vogel** and **Samar**, as applied to claim 8 above, in further view of Applied Cryptography, Second Edition by **Schneier**. Elgamal lacks generating a key, encrypting the key with a client's public key, sending an encrypted key to a client and using the encrypted key to encrypt communications. However, Schneier (page 48, § Key Exchange with Public-Key Cryptography) teaches generating a key/random session key (step 2), encrypting the key with a client's/Bob's public key (step 2), sending an encrypted key to a client/Bob (step 2) and using the encrypted key to encrypt communication (step 4). Schneier teaches that this is a basic key-exchange

scheme used with Public Key cryptography to exchange a session key used to communicate securely (page 48, § Key Exchange with Public-Key Cryptography). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the server to generate a key, encrypt the key with a client's public key, send an encrypted key to a client and use the encrypted key to encrypt communications. One of ordinary skill in the art would have been motivated to perform such a modification to exchange a session key to encrypt communications, as taught by Schneier (page 48, § Key Exchange with Public-Key Cryptography).

10. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Elgamal** in view of **Vogel** and **Samar**, as applied to claim 22 above, in further view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**). Elgamal discloses a system, as modified above, but lacks determining if a client is on an access control list if the authentication is present and valid. However, Menezes teaches that certificates should be revoked if evidence exists that suggests that the certificate should no longer be issued (§13.7.2). Menezes further teaches that certificate authorities publish certificate revocation lists to be checked for invalid certificates (§13.6.3) because distributed copies exist and may not immediately be aware of the need for revocation (§13.6.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine if the client/certificate is on an access control list/certificate revocation list after the authentication token is deemed valid (signature contained in the certificate is successfully decrypted using the public key of the authority and compared to the data over which the signature has been taken). One of ordinary skill in the art would have

been motivated to perform such a modification to make sure the distributed client certificate has been not revoked, as taught by Menezes (§13.6.3 & §13.7.2).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Cryptography Decrypted and Network Security Essentials, Applications and Standards are cited for teaching a general overview of the SSL and TLS protocols, having particular relevance to Applicant's independent claims.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
August 15, 2005